合肥工业大学

# 《信息安全技术》实验报告

# NMAP实验部分

|  |
| --- |
| 姓名 |
| 学号 |
| 专业班级 |

2022年5月

## 一、实验目的

1. 掌握端口扫描这种信息探测技术的原理。

2. 学会使用常见的端口扫描工具。

3. 了解各种常用网络服务所对应的端口号。

## 二、实验内容

1. 使用NMAP的命令行工具进行端口扫描。

2. 使用NMAP的命令行工具进行网络服务。

3. 使用NMAP的命令行工具进行操作系统类型鉴别。

4. 使用NMAP图形化前段Zenmap工具同样进行上述任务。

## 三、实验环境

* 学生实验主机：Window XP
* 实验目标服务器：实验室机房主机 Window Server
* 网络环境：局域网

## 四、实验原理

**端口及服务的基本概念**

“端口”是专门为计算机通信而设计的，在TCPIP协议中规定,用IP地址和端口作为套接字(socket )，代表TCP或UDP通信的一端。端口分为知名(known）端口号和一般端口号，其中知名端口号的数值一般为0~1023，分配给常用应用服务程序固定使用。

**Nmap的功能介绍和技术原理**

Nmap (Network Mapper、网络映射器）是一款开放源代码的网络探测和安全审核的工具。它的设计目标是快速地扫描大型网络，当然用它扫描单个主机也没有问题。Nmap以新颖的方式使用原始IP报文来发现网络上有哪些主机，哪些主机提供什么服务，包括其应用程序名和版本，哪些服务运行在什么操作系统，包括版本信息，它们使用什么类型的报文过滤器/防火墙，以及一堆其它功能。虽然Nmap通常用于安全审核，许多系统管理员和网络管理员也用它来做一些日常的工作，比如查看整个网络的信息，管理服务升级计划，以及监视主机和服务的运行。

Nmap输出的是扫描目标的列表，以及每个目标的补充信息，至于是哪些信息则依赖于所使用的选项。“所感兴趣的端口表格"是其中的关键。状态可能是open(开放的)、filtered(被过滤的)、closed(关闭的)、或者unfiltered(未被过滤的)。

* “Open”意味着目标机器上的应用程序正在该端口监听连接报文。
* “Filtered"意味着防火墙、过滤器或者其它网络障碍阻止了该端口被访问。
* “Closed”意味着没有应用程序在该端口上面监听，但是他们随时可能开放。

当端口对Nmap的探测做出响应，但是Nmap无法确定它们是关闭还是开放时，这些端口就被认为是unfiltered。如果Nmap 报告状态组合open|filtered和 closed|filtered 时，那说明Nmap无法确定该端口处于两个状态中的哪一个状态。当要求进行版本探测时，端口表也可以包含软件的版本信息。当要求进行IP协议扫描时(-sO)，Nmap提供关于所支持的IP协议而不是正在监听的端口的信息。除了所感兴趣的端口表，Nmap还能提供关于目标机的进一步信息，包括反向域名，操作系统猜测，设备类型，和 MAC地址。

**Nmap的基本命令格式如下**

nmap[扫描类型...][选项]{扫描目标说明}

* **主机发现**

任何网络探测任务的最初几个步骤之一就是把一组IP范围缩小为一列活动的或者您感兴趣的主机。扫描每个IP的每个端口很慢，通常也没必要。当然，什么样的主机令您感兴趣主要依赖于扫描的目的。由于主机发现的需求五花八门，Nmap提供了很多的选项来定制您的需求。运行Nmap命令就可以发现主玑发现的一些基本参数，如下列举的部分:

· -sL (列表扫描)：列表扫描是主机发现的退化形式，它仅仅列出指定网络上的每台主机，不发送任何报文到目标主机。

· -sP (Ping扫描)：该选项告诉Nmap仅仅进行ping扫描 (主机发现)，然后打印出对扫描做出响应的那些主机。

· -P0/Pn (无ping)：该选项完全跳过Nmap主机发现阶段，通常Nmap在进行高强度的扫描时用它确定正在运行的机器。

· -PS/PA/PU/PY[portlist]: 使用TCPSYN/ACK或SCTP INIT/ECHO方式进行发现。

· -PE/PP/PM: 使用ICMP echo，timestamp，and netmask 请求包发现主机。

· -n (不用域名解析)：-n表示不进行DNS解析；-R表示总是进行DNS解析。

· --system-dns (使用系统域名解析器)：指定使用系统的DNS服务器。

* **端口扫描**

Nmap把端口分成六个状态: open(开放的)，closed(关闭的)，filtered(被过滤的)，unfiltered(未被过滤的)，open/filtered(开放或者被过滤的)，或者closed|filtered(关闭或者未被过滤的)。

Nmap支持大约十几种扫描技术。一般一次只用一种方法，除了UDP扫描(-sU)可能和任何一种TCP扫描类型结合使用。

· -sS/sT/sA/sW/sM:指定使用TCP SYN/Connect()/ACK/Window/Maimon scans的方式来对目标主机进行扫描。

· -sU: 指定使用UDP扫描方式确定目标主机的UDP端口状况。

· -sN/sF/sX: 指定使用TCP Null, FIN, and Xmas scans秘密扫描方式来协助探测对方的TCP端口状态。

· -sY/sZ: 使用SCTP INIT/COOKIE-ECHO来扫描SCTP协议端口的开放的情况。

· -sO: 使用IP protocol 扫描确定目标机支持的协议类型。

除了所有前面讨论的扫描方法，Nmap提供选项说明那些端口被扫描以及扫描是随机还是顺序进行。默认情况下，Nmap用指定的协议对端口1到1024 以及 nmap-services文件中列出的更高的端口在扫描。

· -p <port ranges>: 只扫描指定的端口。

· -F: 快速 (有限的端口) 扫描。

· -r:不要按随机顺序扫描端口。

* **服务和版本探测**

把Nmap指向一个远程机器，它可能告诉您端口25/tcp，80/tcp，和53/udp是开放的。使用包含大约2,200个著名的服务的nmap-services数据库，Nmap可以报告那些端口可能分别对应于一个邮件服务器(SMTP)，web 服务器(HTTP)，和域名服务器(DNS)。

在用某种其它类型的扫描方法发现TCP和/或者UDP端口后，版本探测会询问这些端口，确定到底什么服务正在运行。nmap-service-probes数据库包含查询不同服务的探测报文和解析识别响应的匹配表达式。Nmap试图确定服务协议(如 ftp，ssh，telnet，http)，应用程序名(如 ISC Bind，Apache httpd，Solaristelnetd)，版本号，主机名，设备类型(如打印机，路由器)，操作系统家族(如 Windows，Linux)以及其它的细节，如是否可以连Xserver，SSH 协议版本，或者KaZaA用户名)。当然，并非所有服务都提供所有这些信息。如果Nmap被编译成支持OpenSSL，它将连接到SSL服务器，推测什么服务在加密层后面监听。当发现RPC服务时，Nmap RPC grinder (-sR)会自动被用于确定RPC程序和它的版本号。

Nmap用下列的选项打开和控制版本探测。

· -sV (版本探测)：打开版本探测，用-A同时打开操作系统探测和版本探测。

· --allports：不为版本探测排除任何端口。

· --version-intensity <intensity> ：设置版本扫描强度。

· --version-light：打开轻量级模式。

* **操作系统类型鉴别**

Nmap最著名的功能之一是用TCPIP协议栈指纹技术(Fingerprinting）进行远程操作系统探测。每个Fingerprint包括一个自由格式的关于OS的描述文本，和一个分类信息，它提供供应商名称(如 Sun),下面的操作系统（如 Solaris),OS版本(如10)，和设备类型（通用设备，路由器，switch，游戏控制台，等）。

操作系统检测可以进行其它一些测试，这些测试可以利用处理过程中收集到的信息。例如运行时间检测，使用TCP时间戳选项(RFC 1323)来估计主机上次重启的时间，这仅适用于提供这类信息的主机。另一种是TCP序列号预测分类，用于测试针对远程主机建立一个伪造的TCP连接的可能难度。

采用下列选项启用和控制操作系统检测:

* -O：启用操作系统检测，也可以使用-A来同时启用操作系统检测和版本检测。

## 五、实验过程

1. 运行实验工具目录下的Nmap安装程序(nmap-5.00-setup.exe)，安装Nmap到系统中的指定路径(C:LiHaoran\Nmap\nmap）。注意:安装过程中保留默认包含的 Winpcap和Zenmap组件，如下图所示。

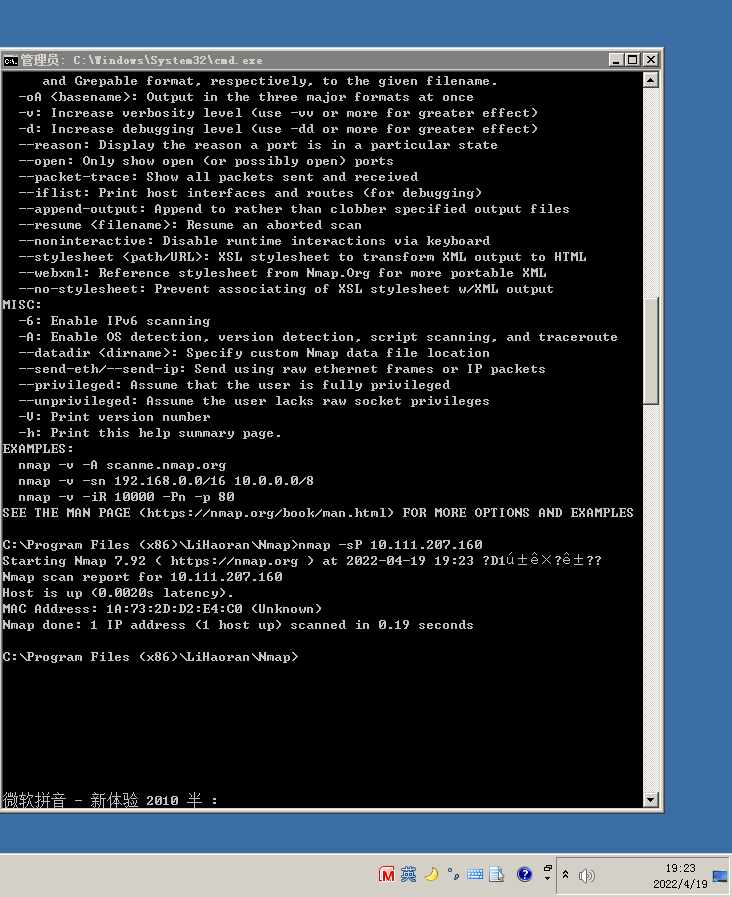


1. 打开系统中的"命令提示符"，进入到Nmap安装路径（指定为“C:LiHaoran\Nmap\nmap”)，运行nmap.exe，查看可用参数。



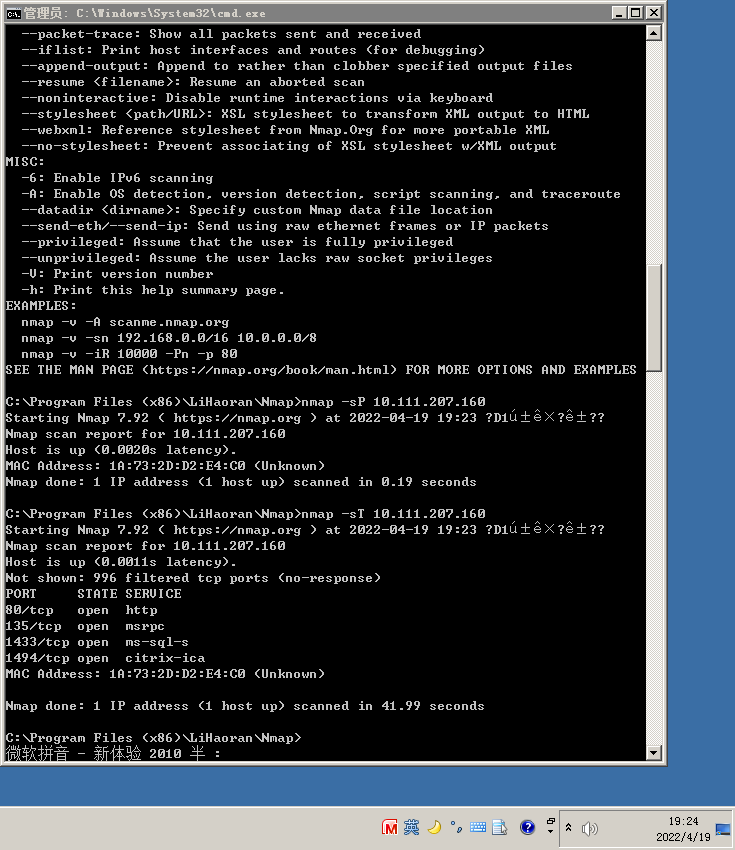
3.主机发现:进行连通性监测，来判断目标主机，机房主机（ip地址为10.111.207.160）是否可连通，运行如下命令:

Nmap -sP 10.111.207.160



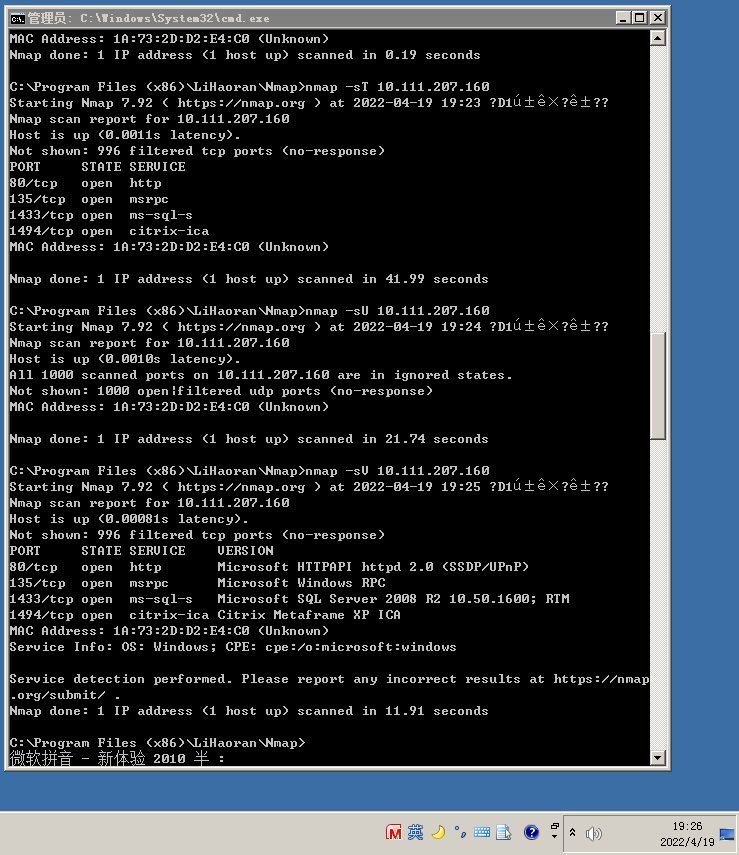
4.使用常规扫描方式对目标主机进行TCP端口扫描，运行如下命令:

Nmap -sT 10.111.207.160



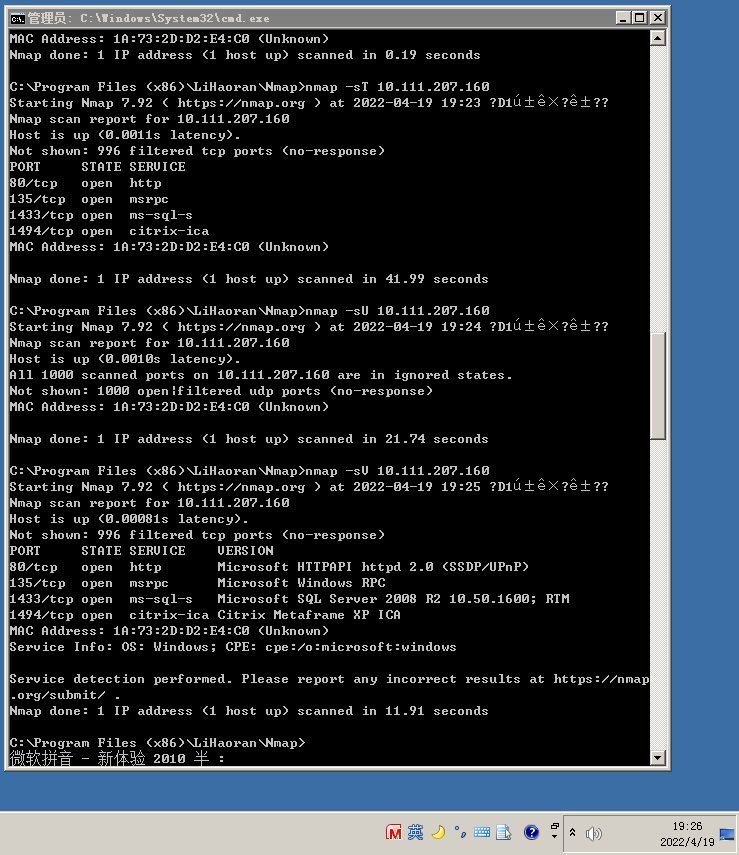
6.对目标主机进行UDP端口扫描，运行如下命令:

Nmap -sU 10.111.207.160



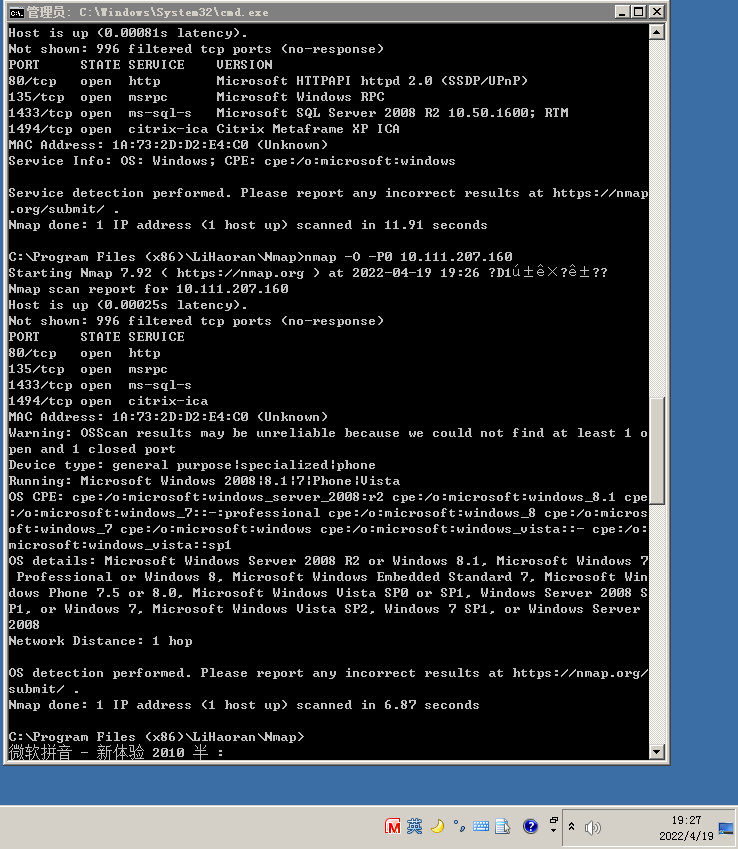
7.探测目标主机主机开放端口上所提供的服务及其类型和版本信息，运行如下命令:

Nmap -sV 10.111.207.160



8.探测目标主机的操作系统类型，运行如下命令:

Nmap -O-P0 10.111.207.160



9.进入到Nmap安装路径（默认为“C:IProgram FilesINmap”)，运行zenmap.exe，即 Nmap 的图形化前端程序。在“Target”文本框中输入扫描目标IP地址/主机名称（192.168.80.201)，然后在“Profile”预定义配置下拉框中选择扫描配置“Intense Scan, no Ping”，然后点击菜单项“Profile"→“Edit Selected Profile”，切换到“Scan”选项卡，勾选上“Operating system detection”和“Versiondetection”后点击“Save Changes”按钮保存扫描配置，最后点击“Scan”按钮开始扫描。

